PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

EXPRESS MAIL NO. EL496231786US

Applicant	:	Michael E. See, et al.
Application No.	:	Not Yet Assigned
Filed	:	May 23, 2001
Title	:	DETERMINISTIC USER AUTHENTICATION SERVICE FOR COMMUNICATION NETWORK
Docket No.	:	41711/SAH/X2

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Post Office Box 7068
Pasadena, CA 91109-7068
June 21, 2001

Commissioner:

Prior to examination of the above-identified application, please amend the application as follows:

IN THE DRAWINGS:

Please amend FIGs 2, 6 and 10 as indicated on the attached redlined drawings sheets.

IN THE SPECIFICATION:

On page 1, after the title and before the heading "FIELD OF THE INVENTION," insert the following:

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. Patent Application No. 09/525,506, filed March 15, 2000, which is a continuation of U.S. Patent Application No. 08/874,054, filed June 13, 1997, now U.S. Patent No. 6,070,243.

On page 1, under the heading FIELD OF THE INVENTION, insert the following:

The present invention relates to regulating connectivity to and within communicability networks. More specifically, the present invention relates to a authenticating and establishing personalized network connectivity for local users of institutional communication networks.

On page 1, under the heading "BACKGROUND OF THE INVENTION", the first paragraph should read as follows:

Institutions are relying increasingly on their data communication network infrastructures for efficient communication and data transfer. With this increasing reliance on network computing has arisen a significant need for mechanisms to regulate connectivity and communicability to and within such networks. This need has been partially filled by interact protocol (IP) firewalls. IP firewalls typically restrict access to fixed sets of network resources by applying a set of protocol level filters on a packet-by-packet basis or by requiring prospective users to become authenticated before gaining access to the resources. Authentication has generally required users to supply certain signature information, such as a password. While this requirement of signature information has reduced the risk of unauthorized access to firewall-protected resources, firewalls have proven an imperfect and inflexible regulatory solution. Because firewalls are protocol-specific, firewalls have not provided a means for regulating network connectivity in a multi-protocol environment. Moreover, because firewalls regulate access to particular network resources, they have failed to provide a means for regulating access to sets of network resources which can vary as a function of user identity.

On page 3, the paragraph beginning on line 18 should read as follows:

Accordingly, there is a need for comprehensive services for regulating communicability in institutional networks which are not subject to the inflexibility of conventional user log-in mechanisms or the lack of consideration for user identity of conventional VLAN assignment techniques. There is also a need for services which authenticate local users of institutional networks before establishing network communicability. There is a further need for user authentication

services which provide collateral functionality, such as the ability to dynamically track the whereabouts of network users.

On page 4, paragraph 2, beginning on line 10, the paragraph should read as follows:

It is therefore one object of the present invention to provide a service which authenticates local users before establishing network communicability.

On page 4, last paragraph beginning on line 21 and continuing through page 5, line 16, should read:

These and other objects of the present invention are accomplished by a service which requires that local users be authenticated before gaining access to personalized sets of network resources. User identification information, time restrictions and authorized lists of resources for particular users are entered and stored in the network. Prior to authentication, packets from an end system being used by a prospective user of network resources are transmitted to an authentication agent operative on an intelligent edge ociated with the system. The agent relays log-in responses received from the system to a basic authentication server in the network for verification of the user. Verification is made by comparing log-in responses with the user identification information stored in the network and determining whether time restrictions associated with the user identification information are applicable. If the basic authentication server is able to verify from the log-in response that the user is an authorized user of network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the basic authentication server transmits to the agent the list of network resources for which the user is authorized, along with any time restrictions. The agent forwards the list of authorized network resources and time restrictions for storage and use on the edge device. The edge device uses the authorized list of resources and time restrictions to establish network communicability rules for the user. Preferably, the authorized list of network resources is a list of one or more VLANs.

Page 6, second paragraph should read as follows:

In another aspect of the invention, when an authenticated user logs-off the network, or fails to transmit packets for a predetermined time, or if the system being used by the authenticated user is disconnected from the network, or if the authorized communicability period expires, or if the basic authentication server or other management entity instructs the agent to abolish the authenticated user's network communicability, the authenticated user's network communicability is deactivated.

Page 12 should read as follows:

Agent 400 also includes RSR.C RLY means 460. Means 460 serves to forward for storage and use on device 10 authorized communicability information received from server 320 for authenticated users of systems 40, 50, 60. Authorized communicability information may advantageously be transmitted by server 320 to agent 400 in the same data packet as user status information. Authorized communicability information includes, for the particular one of the systems 40, 50, 60, a list of authorized network resources. Authorized communicability information may also include time restrictions, if any. Time restrictions preferably define times during which the particular user is authorized to use the network resources, such as the day of the week, the time of day, and the length of permitted access. The list of authorized network resources is preferably a list of VLAN identifiers. Authorized communicability information is preferably forwarded by agent 400 to management processor module 210 along with the authentication module identifier. Management processor module 210 preferably associates the authorized communicability information with a known address of the one of the systems 40, 50, 60 being used by the authenticated user and stores the pair in device records. The address is preferably a MAC address.

Page 13, second sub-paragraph numbered "2" and continuing to page 14, first two paragraphs should read as follows:

2. If the destination address is not the address of another one of systems 40, 50, 60 associated with device 10, resort is made to device records on device 10 to retrieve the VLAN identifiers associated with the source system. The VLAN identifiers are appended to the packet and the packet is transmitted by

backbone module 220 for transmission on backbone network 30. When the packet arrives on the edge device (e.g., 15) associated with the destination system (e.g., 45), resort is made to device records on the edge device to verify that the source and destination systems share a common VLAN. If a VLAN is shared, the packet is forwarded to the destination system. If a VLAN is not shared, the packet is dropped.

Packets addressed to unauthenticated systems in network 1 continue to be dropped. The foregoing rules may be implemented using various known protocols. It will be appreciated that any addressable core, edge, or end devices, stations and systems in network 1 which are not subject to authentication requirements may be treated as authenticated systems for purposes of transmitting and receiving packets under the foregoing rules.

Agent 400 also includes ID TERM means 470. Means 470 serves, upon receipt of log-off commands from authenticated users, or upon expiration of the authorized communicability period, or when one of authenticated systems 40, 50, 60 is physically disconnected from network l, or when one of authenticated systems 40, 50, 60 fails to send traffic for a prescribed length of time, or upon receipt of instruction from server 320, to deactivate the established network communicability. Means 460 forwards to management processor module 2 l0 a request to remove from device records the address-authorized connectivity information entry for the user whose connectivity is to be deactivated. Upon receipt of such a request, management processor module 210 preferably removes the entry from device records and the authenticated one of systems 40, 50, 60 reverts to the unauthenticated state.

Tuming to Fig. 5, a functional diagram of basic authentication server 320 is shown. Server 320 includes RSRC AUTH means 510. Means 510 serves to enable network administrators to define, on an individualized basis, authorized communicability.....

Pages 16 and 17 are amended to read as follows:

Server 320 also includes ID VER means 530. Means 530 serves to subject to a verification process authentication information received from users via agent 400. Means 530, upon receipt of

authentication information from agent 400, determines if the log-in response matches the user identification information associated with a user-specific entry in user records 330. If a match is found, and there are time restrictions associated with the user-specific entry, means 530 determines from the time restrictions if the user is authorized to use network 1 at the particular time. If the user is time-authorized or there are no time restrictions, means 530 generates authorized communicability information. Means 530 retrieves the list of authorized network resources associated with the matching user identification information in the generation of authorized communicability information. Authorized communicability information may also include any time restrictions. Means 530 also generates user status information. User status information is information sufficient to communicate to agent 400 whether user identification information was successfully verified. User status information is preferably either a log-in valid or log-in invalid message. Means 530 transmits authorized communicability information and user status information to agent 400. Preferably, authorized communicability information and user status information are transmitted as part of the same data packet. If no match for user identification information is found, or if the user is not time-authorized, means 530 generates and transmits to agent 400 user status information, preferably in the form of a log-in invalid message, but does not generate or transmit authorized communicability information. Although the above described means operative on server 320 are described to be interoperative in conjunction with agent 400, it will be appreciated that the means are fully interoperative with other authentication agents residing on edge devices in network 1.

Server 320 also includes ID STOR means 540. Means 540 serves to forward for storage and use by a network administrator user tracking information. User tracking information is preferably retained for all log-in attempts made by prospective users, whether successful or unsuccessful. User tracking information may include, for each log-in attempt, any information learned from one or more of the following: user identification information, authentication information, user status information, authorized communicability information. User tracking information also may include the time of day the log-in attempt was made. The time of day may be kept on and obtained from server 320. Server 320 preferably associates the user tracking information and stores the information as an entry in a

network activity database (not shown) that is accessible by or resides on station 20. Network activity database entries are accessible by a network administrator using interface 310.

Server 320 also includes NET MNTR means 550. Means 550 serves to enable a network administrator to access and use user tracking information. Means 550 supplies a textual or graphical display to interface 310 operative to display user tracking information. Means 550 also enables a network administrator to generate user tracking information reports consisting of related information from one or more user tracking information entries.

Client 360 further includes ID OFF means 640. Means 640 serves to initiate the log-off process by which authenticated users log-off the network 1. Means 640 supplies a textual or graphical display to user interface 350 operative to accept log-off commands. Means 640 transmits log-off commands to agent 400 for deactivation of established network connectivity.

The last paragraph on page 18 is amended to read as follows:

Referring to Fig. 7, a network 7 operating in accordance with an alternative embodiment of the present invention is shown. In the alternative embodiment, an enhanced authentication method is conducted before network communicability is granted.

The last paragraph beginning on page 20 and continuing through the last paragraph on page 21 should read as follows:

Server 800 also includes ENH ID VER means 830. Means 830 serves, upon verifying log-in responses received from a user and that the user is authorized to use the network 7 at the time of the log-in attempt, to initiate an enhanced authentication method, if indicated. Means 830, upon determining that the log-in response matches user identification information associated with a user-specific entry in user records, and upon determining that the user is time-authorized if time restrictions are indicated, checks whether there is an enhanced authentication method associated with the matching user-specific entry. If an enhanced authentication method is indicated, means 820, before transmitting authorized communicability information and user status information to the agent on the appropriate one of devices 7.10, 715, transmits a request to enhanced authentication server

770 to conduct an enhanced authentication session with the user. The enhanced authentication session is preferably conducted between enhanced server 770 and the user transparently to basic server 800. Enhanced server 770 instructs basic server 800 of the results of the enhanced authentication session. If the user was successfully authenticated, means 830 transmits to the agent authorized communicability information and user status information, preferably in the form of a log-in valid message. If the user was not successfully authenticated, means 830 transmits user status information, preferably a log-in invalid message, but no authorized communicability information. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed, means 830 transmits to the agent authorizedcommunicability information and user status information, in the form of a log-in valid message, without engaging server 770. If a matching entry for user identification information is not found in user records, or if the user is not time-authorized, means 830 transmits to the agent user status information, in the form of a log-in invalid message, without transmitting authorized communicability information.

The first paragraph on page 23 is amended as follows:

Accordingly, once a determination is made that the user is time-authorized (1005), basic server 800 checks whether there is an enhanced authentication method associated with the matching entry (1010). If an enhanced authentication method is indicated, server 800 transmits a request to enhanced authentication server 770 to conduct an enhanced authentication session with the user (1015). Enhanced server 770 informs basic server 800 of the results of the enhanced authentication session. If the session was successfully completed (1020), basic server 800 transmits authorized communicability information and user status information, in the form of a log-in valid message, to the agent (1030). If enhanced session was not successfully completed (1025), basic server 800 transmits a log-in invalid message to user and does not transmit authorized communicability information to agent. Agent also in that instance determines if user has made a configurable number of failed log-in attempts. The authentication session either continues or terminates as discussed depending on the outcome of that inquiry. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed (1010), server 800 transmits

authorized communicability information and user status information, in the form of a log-in valid message, without requesting server 770 to conduct an enhanced authentication session.

IN THE CLAIMS:

Please cancel claims 1-43 and add new claims 44-114 as follows:

44. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein the end-node is authorized based at least in part on the verification of the user information to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

45. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to the verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

46. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

47. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the end-node accesses the edge node via the interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node and other nodes in the institutional LAN.

48. The edge node of claim 47, wherein the interface reverts to the unauthenticated state if a packet is not received from the end-node for a predetermined time period.

49. The edge node of claim 47, wherein the interface reverts to the unauthenticated state upon detecting that the end-node has become disconnected.

50. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from an end-node via a LAN link for verification,

wherein the end-node accesses the edge node via a LAN interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

51. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the end-node accesses the edge node via the interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

52. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node to an institutional LAN including verifying the user information.

53. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node including verifying the user information and performing LAN media translations.

54. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node including verifying the user information and performing LAN switching based at least in part on MAC addresses.

55. An authentication agent for representing an edge node in an authentication protocol exchange with an end-node for access to an institutional LAN, the agent comprising:

means for transmitting a request for user information via a LAN link to the end-node;

means for receiving user information from the end-node via a LAN link in response to the request;

means for transmitting the user information to an authentication server for verification;

means for receiving verification information from the authentication server at least in part in response to the user information; and

means for regulating access of the end-node to services of the institutional LAN available through the edge node in response to the verification information.

56. The authentication agent of claim 55, wherein the authentication agent is a software program.

57. The authentication agent of claim 55, wherein the authentication agent is resident on the edge node.

58. The authentication agent of claim 55, wherein the authentication agent further includes means for transmitting the verification information to the end-node.

59. A system for authorizing an end-node to a LAN infrastructure, the system comprising:

an edge node; and

an interface associated with the edge node for receiving authentication information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to

the edge node that the authentication information has been verified, whereupon the end-node is authorized for access to services of a LAN infrastructure via the edge node.

60. The system of claim 59, wherein the authentication server is a RADIUS server.

61. A user authentication system comprising:

an edge node;

an interface on the edge node for receiving a authentication information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node;

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the edge node that the authentication information has been verified, whereupon the edge node is authorized to provide LAN switching functions for packet flows involving the end-node.

62. The system of claim 61, wherein the authentication server is a RADIUS server.

63. The system of claim 61, wherein the LAN switching functions include forwarding and filtering packets in function of MAC addresses.

64. The system of claim 61, wherein the LAN switching functions include performing LAN media translations on the packets.

65. An authentication system for authorizing an end-node, the system comprising:

an edge node;

an interface on the edge node for receiving a authentication information from the end-node via a LAN link for verification; and

an authentication server coupled to the edge node;

wherein a message exchange between the edge node and the authentication server is conducted to verify the authentication information, whereupon the end-node is authorized for access to services of a LAN infrastructure via the edge node, and

wherein a security protocol is applied to secure the message exchange between the edge node and the authentication server.

66. An authentication system for authorizing an end-node, the system comprising:

a LAN interface for receiving user information from the end-node via a LAN link;

an authentication agent for receiving the user information from the LAN interface via a switching link;

a backbone interface for receiving the user information from the authentication agent via the switching link; and

an authentication server for receiving the user information from the backbone interface for verification,

wherein prior to verification of the user information the LAN interface transmits on the switching link packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the LAN interface is authorized to transmit on the switching link packets in data flows involving the end-node.

67. An authentication system for authorizing an end-node, the system comprising:

an edge node;

an interface associated with the edge node for managing interactions on a LAN link with the end-node in an authentication protocol exchange; and

an authentication server coupled to the edge node;

wherein the edge node forwards information concerning the authentication protocol exchange to the authentication server in response to which the authentication server generates and stores in a database tracking information concerning the authentication protocol exchange.

68. The system of claim 67, wherein the tracking information includes user information.

69. The system of claim 67, wherein the tracking information includes network location information.

70. The system of claim 67, wherein the tracking information includes time-of-day information.

71. A method for representing an edge node in an authentication protocol exchange with an end-node for access to an institutional LAN, the method comprising:

transmitting a request for user information via a LAN link to the end-node;

receiving user information from the end-node via the LAN link in response to the request;

transmitting the user information to an authentication server for verification;

receiving verification information from the authentication server at least in part in response to the user information; and

regulating access of the end-node to services of the institutional LAN available through the edge node in response to the verification information.

72. The method of claim 71 further comprising the step of transmitting the verification information to the end-node.

73. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and

wherein at least in part in response to the verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

74. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node;

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

75. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein prior to verification of the user information the end- node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

76. A user authentication system for an institutional LAN having an edge node with a first interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node.

77. The system of claim 76, wherein the first interface reverts to the unauthenticated state if a packet is not received from the end-node for a predetermined time period.

78. The system of claim 77, wherein the first interface reverts to the unauthenticated state upon detecting that the end-node has become disconnected.

79. A user authentication system for an institutional LAN having an edge node with a first interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

80. A user authentication system for an institutional LAN having an edge node with a first

interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

81. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the end-node is authorized to send and receive through the edge node packets in data flows involving the end-node only after verification of the user information.

82. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the edge node regulates packet flows from the end-node including subjecting the user information to verification and performing LAN media translations.

83. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the edge node regulates packet flows from the end-node including subjecting the user information to verification and performing LAN switching based at least in part on MAC addresses.

84. An authentication client for representing an end-node in an authentication protocol exchange with an edge node coupled to the end-node via a LAN link to obtain access for the end-node to services of an institutional LAN available through the edge node, the client comprising:

means for receiving a request for user information from the edge node; and

means for transmitting user information to the edge node in response to the request.

85. The authentication client of claim 84, wherein the authentication client is a software program.

86. The authentication client of claim 84, wherein the authentication client is resident on the end-node.

87. The authentication client of claim 84, further comprising means for receiving a request for second user information from the edge node in response to the user information.

88. The authentication client of claim 87, further comprising means for transmitting the second user information to the edge node in response to the request for second user information.

89. The authentication client of claim 88, further comprising means for receiving verification information from the edge device in response to the second user information.

90. The authentication client of claim 84, wherein the end-node is a personal computer.

91. The authentication client of claim 84, further comprising means for receiving verification information from the edge device in response to the user information.

92. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the edge node that the authentication information has been verified, whereupon the end-node is authorized for access to services of a LAN infrastructure via the edge node.

93. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the edge node that the authentication information has been verified, whereupon the edge node is authorized to provide LAN switching functions for packet flows involving the end-node.

94. The system of claim 93, wherein the LAN switching functions include forwarding and filtering in function of MAC addresses.

95. The system of claim 93, wherein the LAN switching functions include LAN media translations.

96. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein a message exchange between the edge node and the authentication server is conducted to verify the authentication information, whereupon the end-node is authorized for access to services of an institutional LAN via the edge node, and

wherein a security protocol is applied to secure the message exchange between the edge node and the authentication server.

97. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for managing interactions with the user in an authentication protocol exchange and a LAN interface for managing interactions on a LAN link with the edge node in the authentication protocol exchange,

wherein the edge node forwards information concerning the authentication protocol exchange to the authentication server in response to which the authentication server generates and stores in a database tracking information concerning the authentication protocol exchange.

98. The system of claim 97, wherein the tracking information includes user information.

99. The system of claim 97, wherein the tracking information includes network location information.

100. The system of claim 97, wherein the tracking information includes time-of-day information.

101. A method for representing an end-node in an authentication protocol exchange with an edge node coupled to the end-node via a LAN link to obtain access for the end-node to services of an institutional LAN available through the edge node, the method comprising:

receiving a request for user information from the edge node; and

transmitting user information to the edge node in response to the request.

102. The method of claim 101, further comprising the step of receiving first verification information from the edge node in response to the user information.

103. The method of claim 102, further comprising the step of receiving a request for second user information from the edge node in response to the first verification information.

104. The method of claim 103, further comprising the step of transmitting second user information to the edge node in response to the request for second user information.

105. The method of claim 104, further comprising the step of receiving second verification information from the edge device in response to the second user information.

106. An authentication system for authorizing an end-node to an institutional LAN, the system comprising:

an edge node having an interface for receiving a first response containing first user information and second response containing second user information from the end-node via a LAN link for verification, and

wherein prior to verification of the second user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein the end-node is authorized in response to the verification of the second user information to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

107. The system of claim 106 wherein the second user information is received after verification of the first user information.

108. The system of claim 106, further comprising an authentication server coupled to the edge node wherein the edge node transmits the second user information to the authentication server, and the second authentication server verifies the second user information.

109. A user authentication system for authorizing an end-node to an institutional LAN, the system comprising:

an edge node having an interface for receiving first user information and second user information from the end-node via a LAN link for verification,

wherein the edge node causes verification of the first user information, and upon verification of the first user information, the edge node receives and causes verification of the second user information, and

wherein in response to verification of the second user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node and other nodes in the institutional LAN.

110. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving first user information and second user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node to an institutional LAN including causing verification of the first user information and second user information.

111. A system for accessing an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting first authentication information and second authentication information via a LAN link to the edge node for verification,

wherein the end-node is initially authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein in response to the verification of the second authentication information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

112. A method for authorizing an end-node to an institutional LAN having a plurality of nodes including an edge node, the method comprising:

enabling an authentication flow between the end-node and the edge node via a LAN link;

receiving first authentication information from the end-node;

performing a first verification attempt on the first authentication information;

depending upon a result of the first verification attempt, soliciting or not second authentication information from the end-node;

performing a second verification attempt on the second authentication information; and

depending upon a result of the second verification attempt, authorizing or not the end-node to transmit and receive through the edge node packets in data flows involving the end-node and the other nodes in the institutional LAN.

113. A method for authorizing an end-node to an institutional LAN having a plurality of nodes including an edge node, the method comprising:

transmitting from the end-node to the edge node via a LAN link first user information;

receiving a request for second user information upon verification of the first user information;

transmitting the second user information in response to the request;

obtaining, upon verification of the second user information, authorization to transmit and receive through the edge node packets in data flows involving the end-node and the other nodes in the institutional LAN.

114. The method of claim 86, further comprising the step of performing LAN media translations within the edge node on packets transferred by the end-node through the edge node after the second comparison.

REMARKS

By this amendment, Applicants have made corrections to the drawings and the specification and have added new claims 44-114. The amendments to the drawings and the specification add no new matter and have been previously approved by the Examiner in the connection with the applications from which the present application claims priority. More particularly, in the drawings, Applicants have amended FIG. 2 to show an interconnection between the switching link 230 and the backbone module (BM) 220. No new matter has been added in FIG. 2 since the interconnection between link 230 and BM 220 is disclosed on page 8, lines 19 through 22, of the specification. Applicants have amended FIG. 6 to correct a reference numeral and have amended FIG. 10 to add "Y" below step 1005 to indicate a decision. No new matter has been added to FIG. 10, as the insertion of "Y" is disclosed in lines 5 through 7 on page 23 of the specification.

In the specification, Applicants have added a section cross-referencing related applications to add the number of the issued U.S. patent corresponding to the application from which the present application claims priority. Applicants have also deleted a reference in the specification to an issued patent and an application that merely provides one or two examples of the wide variety of protocols known by those of ordinary skill in the art. The remaining changes of the word "connectivity" to "communicability," which were made and approved in the applications from which the present application claims priority, are also made here for consistency.

Based on the foregoing, Applicants respectfully request entry of the present amendment and examination and allowance of this application.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "**Version with markings to show changes made.**"

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Art Hasan
Reg. No. 41,057
626/795-9900

SAH/jhg

VERSION WITH MARKINGS TO SHOW CHANGES MADE

FIELD OF THE INVENTION

The present invention relates to regulating connectivity to and **communicability** within communication networks. More specifically, the present invention relates to authenticating and establishing personalized network connectivity for local users of institutional communication networks.

BACKGROUND OF THE INVENTION

Institutions are relying increasingly on their data communication network infrastructures for efficient communication and data transfer. With this increasing reliance on network computing has arisen a significant need for mechanisms to ~~[regulateconnectivity]~~ **regulate connectivity** to and **communicability** within such networks. This need has been partially filled by interact protocol (IP) firewalls. IP firewalls typically restrict access to fixed sets of network resources by applying a set of protocol level filters on a packet-by-packet basis or by requiring prospective users to become authenticated before gaining access to the resources. Authentication has generally required users to supply certain signature information, such as a password. While this requirement of signature information has reduced the risk of unauthorized access to firewall-protected resources, firewalls have proven an imperfect and inflexible regulatory solution. Because firewalls are protocol-specific, firewalls have not provided a means for regulating network connectivity in a multi-protocol environment. Moreover, because firewalls regulate access to particular network resources, they have failed to provide a means for regulating access to sets of network resources which can vary as a function of user identity.

Accordingly, there is a need for comprehensive services for regulating ~~[connectivity]~~ **communicability** in institutional networks which are not subject to the inflexibility of conventional user log-in mechanisms or the lack of consideration for user identity of ~~[]~~conventional VLAN assignment techniques. ~~[authenticate local users of institutional connectivity.]~~There is also a need for services which **authenticate local users of institutional** networks before establishing network **communicability.** There is a further need for user authentication services which provide collateral functionality, such as the ability to dynamically track the whereabouts of network users.

These and other objects of the present invention are accomplished by a service which requires that local users be authenticated before gaining access to personalized sets of network resources. User identification information, time restrictions and authorized lists of resources for particular users are entered and stored in the network. Prior to authentication, packets from an end system being used by a prospective user of network resources are transmitted to an authentication agent operative on an intelligent edge with the system. The agent relays log-in responses received from the ~~[]~~system to a basic authentication server in the network for verification of the user. Verification is made by comparing log-in responses with the user identification information stored in the network and determining whether time restrictions associated with the user identification information are applicable. If the basic authentication server is able to verify from the log-in response that the user is an authorized user of network resources, and that the user is authorized to use the network resources at the time of the log-in attempt, the basic authentication server transmits to the agent the list of network resources for which the user is authorized, along with any time restrictions. The agent forwards the list of authorized network resources and time restrictions for storage and use on the

edge device. The edge device uses the authorized list of resources and time restrictions to establish network ~~[connectivity]~~ **communicability** rules for the user. Preferably, the authorized list of network resources is a list of one or more VLANs.

In another aspect of the invention, when an authenticated user logs-off the network, or fails to transmit packets for a predetermined time, or if the system being used by the authenticated user is disconnected from the network, or if the authorized ~~[connectivity]~~ **communicability** period expires, or if the basic authentication server or other management entity instructs the agent to abolish the authenticated user's network ~~[connectivity]~~ **communicability**, the authenticated user's network ~~[connectivity]~~ **communicability** is deactivated.

Agent 400 also includes RSR.C RLY means 460. Means 460 serves to forward for storage and use on device 10 authorized ~~[connectivity]~~ **communicability** information received from server 320 for authenticated users of systems 40, 50, 60. Authorized ~~[connectivity]~~ **communicability** information may advantageously be transmitted by server 320 to agent 400 in the same data packet as user status information. Authorized ~~[connectivity]~~ **communicability** information includes, for the particular one of the systems 40, 50, 60, a list of authorized network resources. Authorized ~~[connectivity]~~ **communicability** information may also include time restrictions, if any. Time restrictions preferably define times during which the particular user is authorized to use the network resources, such as the day of the week, the time of day, and the length of permitted access. The list of authorized network resources is preferably a list of VLAN identifiers. Authorized ~~[connectivity]~~ **communicability** information is preferably forwarded by agent 400 to management processor module 210 along with the authentication module identifier. Management processor module 210

preferably associates the authorized ~~[connectivity]~~ **communicability** information with a known address of the one of the systems 40, 50, 60 being used by the authenticated user and stores the pair in device records. The address is preferably a MAC address.

2. If the destination address is not the address of another one of systems 40, 50, 60 associated with device 10, resort is made to device records on device 10 to retrieve the VLAN identifiers associated with the source system. The VLAN identifiers are appended to the packet and the packet is ~~[forwarded to]~~ **transmitted by** backbone module 220 for transmission on backbone network 30. When the packet arrives on the edge device (e.g., 15) associated with the destination system (e.g., 45), resort is made to device records on the edge device to verify that the source and destination systems share a common VLAN. If a VLAN is shared, the packet is forwarded to the destination system. If a VLAN is not shared, the packet is dropped.

Packets addressed to unauthenticated systems in network 1 continue to be dropped. The foregoing rules may be implemented using various known protocols. ~~[See, e.g., Ross U.S. Patent No. 5,394,402 and Nair & Bailey, Application Serial No. 08/782,444, which are incorporated herein by reference.]~~ It will be appreciated that any addressable core, edge, or end devices, stations and systems in network 1 which are not subject to authentication requirements may be treated as authenticated systems for purposes of transmitting and receiving packets under the foregoing rules.

Agent 400 also includes ID TERM means 470. Means 470 serves, upon receipt of log-off commands from authenticated users, or upon expiration of the authorized ~~[connectivity]~~

communicability period, or when one of authenticated systems 40, 50, 60 is physically disconnected from network 1, or when one of authenticated systems 40, 50, 60 fails to send traffic for a prescribed length of time, or upon receipt of instruction from server 320, to deactivate the established network ~~[connectivity]~~ **communicability**. Means 460 forwards to management processor module 2 10 a request to remove from device records the address-authorized connectivity information entry for the user whose connectivity is to be deactivated. Upon receipt of such a request, management processor module 210 preferably removes the entry from device records and the authenticated one of systems 40, 50, 60 reverts to the unauthenticated state.

Turning to Fig. 5, a functional diagram of basic authentication server 320 is shown. Server 320 includes RSRC AUTH means 510. Means 510 serves to enable network administrators to define, on an individualized basis, authorized ~~[connectivity]~~ **communicability.**

Server 320 also includes ID VER means 530. Means 530 serves to subject to a verification process authentication information received from users via agent 400. Means 530, upon receipt of authentication information from agent 400, determines if the log-in response matches the user identification information associated with a user-specific entry in user records 330. If a match is found, and there are time restrictions associated with the user-specific entry, means 530 determines from the time restrictions if the user is authorized to use network 1 at the particular time. If the user is time-authorized or there are no time restrictions, means 530 generates authorized ~~[connectivity]~~ **communicability** information. Means 530 retrieves the list of authorized network resources associated with the matching user identification information in the generation of authorized ~~[connectivity]~~ **communicability** information. Authorized ~~[connectivity]~~ **communicability**

information may also include any time restrictions. Means 530 also generates user status information. User status information is information sufficient to communicate to agent 400 whether user identification information was successfully verified. User status information is preferably either a log-in valid or log-in invalid message. Means 530 transmits authorized ~~[connectivity]~~ **communicability** information and user status information to agent 400. Preferably, authorized ~~[connectivity]~~ **communicability** information and user status information are transmitted as part of the same data packet. If no match for user identification information is found, or if the user is not time-authorized, means 530 generates and transmits to agent 400 user status information, preferably in the form of a log-in invalid message, but does not generate or transmit authorized ~~[connectivity]~~ **communicability** information. Although the above described means operative on server 320 are described to be interoperative in conjunction with agent 400, it will be appreciated that the means are fully interoperative with other authentication agents residing on edge devices in network 1.

Server 320 also includes ID STOR means 540. Means 540 serves to forward for storage and use by a network administrator user tracking information. User tracking information is preferably retained for all log-in attempts made by prospective users, whether successful or unsuccessful. User tracking information may include, for each log-in attempt, any information learned from one or more of the following: user identification information, authentication information, user status information, authorized ~~[connectivity]~~ **communicability** information. User tracking information also may include the time of day the log-in attempt was made. The time of day may be kept on and obtained from server 320. Server 320 preferably associates the user tracking information and stores the information as an entry in a network activity database (not shown) that is accessible by or resides on station 20.

Network activity database entries are accessible by a network administrator using interface 310.

Server 320 also includes NET MNTR means 550. Means 550 serves to enable a network administrator to access and use user tracking information. Means 550 supplies a textual or graphical display to interface 310 operative to display user tracking information. Means 550 also enables a network administrator to generate user tracking information reports consisting of related information from one or more user tracking information entries.

Client 360 further includes ID OFF means 640. Means 640 serves to initiate the log-off process by which authenticated users log-off the network 1. Means 640 supplies a textual or graphical display to user interface 350 operative to accept log-off commands. Means 640 transmits log-off commands to agent 400 for deactivation of established network connectivity.

Referring to Fig. 7, a network 7 operating in accordance with an alternative embodiment of the present invention is shown. In the alternative embodiment, an enhanced authentication method is conducted before network ~~[connectivity]~~ **communicability** is granted.

Server 800 also includes ENH ID VER means 830. Means 830 serves, upon verifying log-in responses received from a user and that the user is authorized to use the network 7 at the time of the log-in attempt, to initiate an enhanced authentication method, if indicated. Means 830, upon determining that the log-in response matches user identification information associated with a user-specific entry in user records, and upon determining that the user is time-authorized if time restrictions are indicated, checks whether there is an enhanced authentication method associated with the matching user-specific entry. If an enhanced authentication method is indicated, means 820, before transmitting authorized ~~[connectivity]~~ **communicability** information and user status

information to the agent on the appropriate one of devices 7.10, 715, transmits a request to enhanced authentication server 770 to conduct an enhanced authentication session with the user. The enhanced authentication session is preferably conducted between enhanced server 770 and the user transparently to basic server 800. Enhanced server 770 instructs basic server 800 of the results of the enhanced authentication session. If the user was successfully authenticated, means 830 transmits to the agent authorized ~~[connectivity]~~ **communicability** information and user status information, preferably in the form of a log-in valid message. If the user was not successfully authenticated, means 830 transmits user status information, preferably a log-in invalid message, but no authorized ~~[connectivity]~~ **communicability** information. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed, means 830 transmits to the agent ~~[authorized connectivity]~~ authorized **communicability** information and user status information, in the form of a log-in valid message, without engaging server 770. If a matching entry for user identification information is not found in user records, or if the user is not time-authorized, means 830 transmits to the agent user status information, in the form of a log-in invalid message, without transmitting authorized **communicability** information.

Accordingly, once a determination is made that the user is time-authorized (1005), basic server 800 checks whether there is an enhanced authentication method associated with the matching entry (1010). If an enhanced authentication method is indicated, server 800 transmits a request to enhanced authentication server 770 to conduct an enhanced authentication session with the user (1015). Enhanced server 770 informs basic server 800 of the results of the enhanced authentication session. If the session was successfully completed (1020), basic server 800 transmits authorized

~~[connectivity]~~ **communicability** information and user status information, in the form of a log-in valid message, to the agent (1030). If enhanced session was not successfully completed (1025), basic server 800 transmits a log-in invalid message to user and does not transmit authorized ~~[connectivity]~~ **communicability** information to agent. Agent also in that instance determines if user has made a configurable number of failed log-in attempts. The authentication session either continues or terminates as discussed depending on the outcome of that inquiry. If an enhanced authentication method is not indicated when the check for an enhanced authentication method is performed (1010), server 800 transmits authorized ~~[connectivity]~~ **communicability** information and user status information, in the form of a log-in valid message, without requesting server 770 to conduct an enhanced authentication session.

JHG PAS352530.1-*-5/23/01 3:51 PM